Office of Information Security
OCIO

Information Security Officer Meeting

September 10, 2009

Office of Information Security
OCIO

Reaching Us…

- Main number – (916) 445-5239
- Change to email addresses
  - security@**state**.ca.gov
  - mark.weatherford@**state**.ca.gov
  - patrick.mcguire@**state**.ca.gov
  - michele.robinson@**state**.ca.gov
  - katrina.yang@**state**.ca.gov
- Office closures due to mandated furloughs
- New Web Site – stay tuned

Office of Information Security
OCIO

OCIO/OIS
Organizational Update

- GRP Transition
- OIS Vacancies and recruitment efforts
- Impact on OIS' ability to meet prior service level expectations
- Also on the move…

Office of Information Security
OCIO

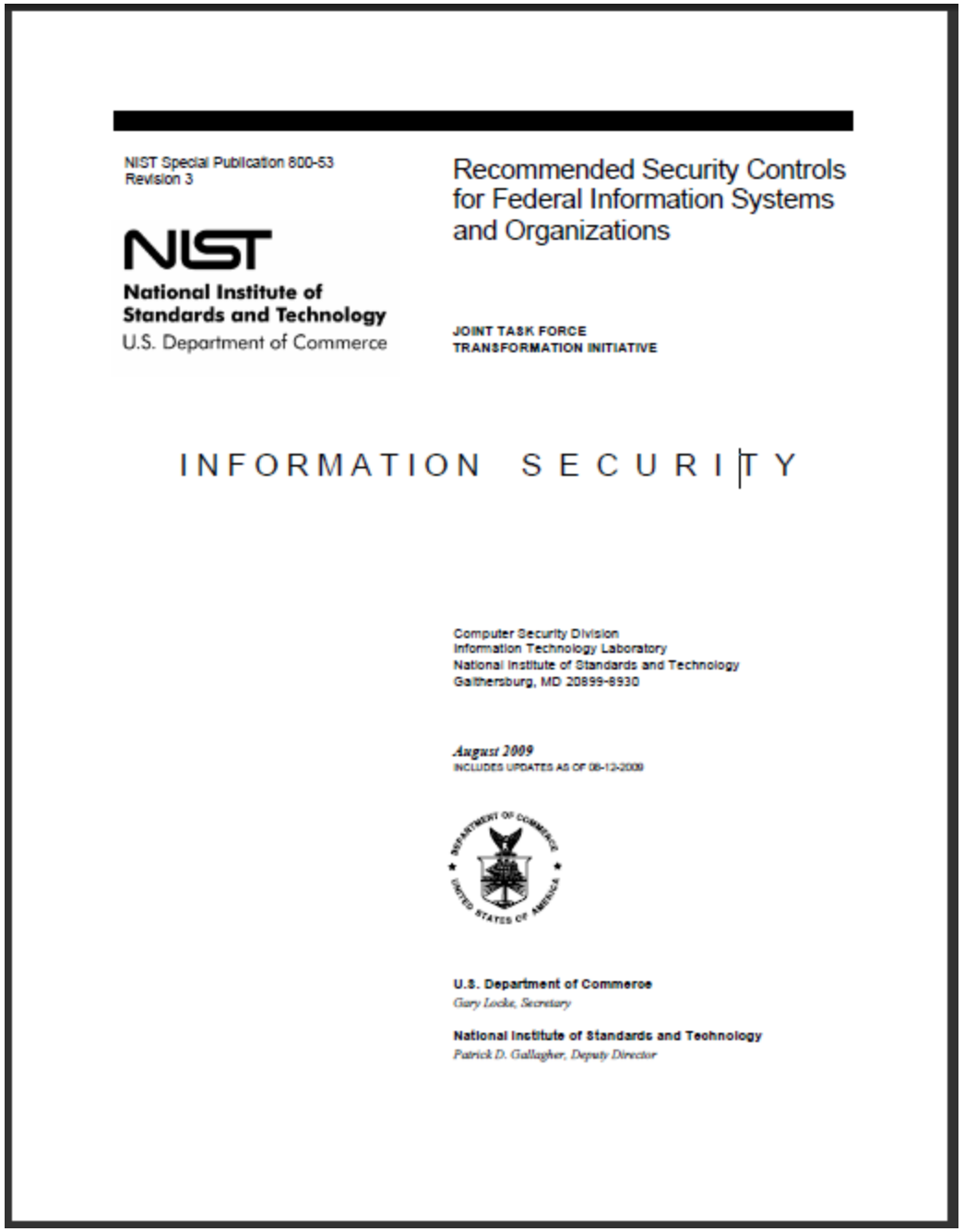
Today's Agenda

- NIST 800-53A
- Is your phone system secure
- IT Capital Plan – Security Survey
- October is Cyber-security Month
- California's Security Strategic Plan
- Incident Management
- Grant Funding
- New Information Security Policy

Office of Information Security
OCIO

NIST SP 800-53

- Clean up
- New Family
- Better Organized
- Focus on Risk
- The Security Professional's Swiss Army Knife



NIST Special Publication 800-53
Revision 3

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Recommended Security Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

August 2009
INCLUDES UPDATES AS OF 08-12-2009

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Deputy Director

Office of Information Security
OCIO

NIST SP 800-53

- Not Standalone
- A tool used with:
  - -- SAM
  - -- Gov. Code
  - -- FIPS
  - -- Other Special Publications

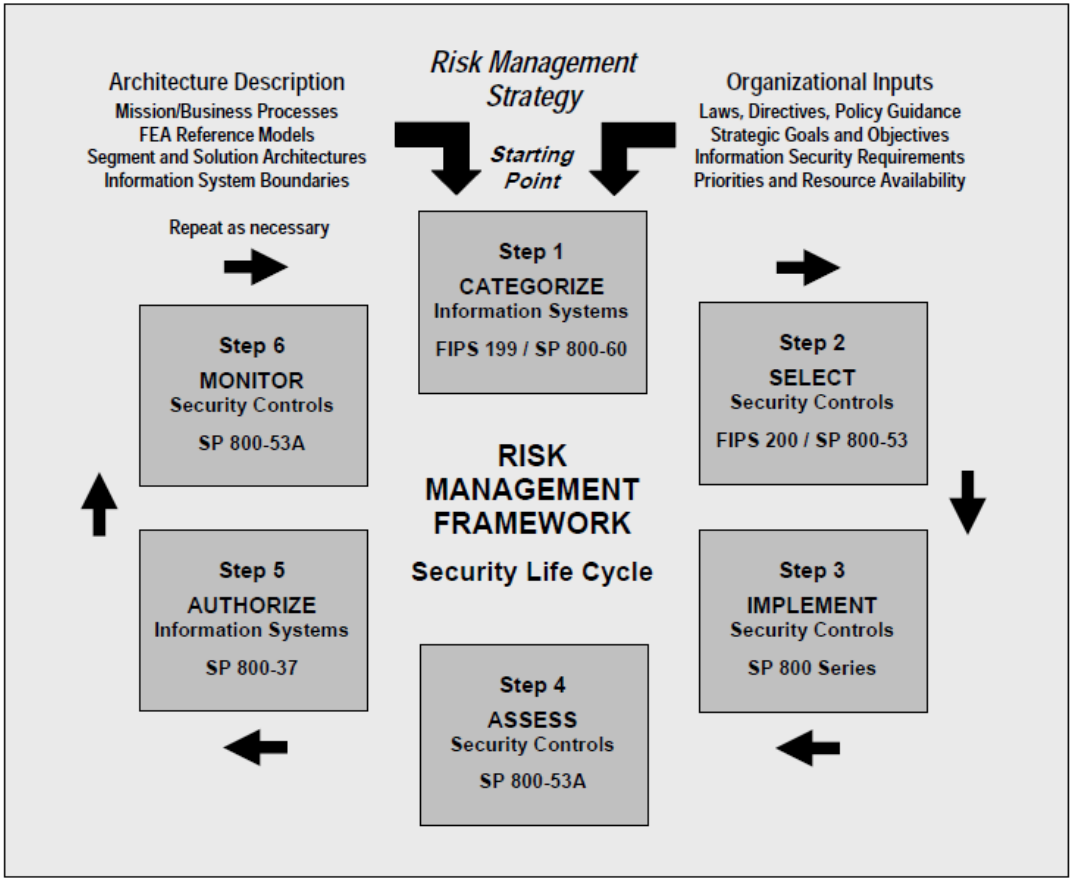


FIGURE 3-1: RISK MANAGEMENT FRAMEWORK

Office of Information Security

OCIO

Is Your PBX/Phone System Secure?

AT&T

PBX SECURITY: IT'S YOUR BUSINESS

PBX (Private Branch Exchange) Security

A PBX is a private switch that serves extensions in a business and provides access to the public switched network. If the PBX system is not maintained and secured, it can be an easy target for those with a mind to commit toll fraud.

PBX and Voice Mail Security Tips

❑ Run periodic security audits to check for loopholes in the PBX (have PBX vendor do this if possible)
❑ Disable DISA (*Direct Inward System Access*) if possible. If not possible, use maximum number of digits for DISA code.
❑ Eliminate remote access to your PBX and disable access system. Have authorized personnel use calling cards instead, if practical.
❑ Do not allow unlimited attempts to enter system. Program PBX to terminate access after third invalid attempt.
❑ Shred directories or anything listing PBX access numbers.
❑ Never divulge system information unless you know to whom you are giving it.
❑ Secure remote maintenance port and use call back modem or alphanumeric passwords.
❑ Tailor access to the PBX to conform to business needs.
❑ Eliminate trunk to trunk transfer capability.
❑ Restrict 0+, 0- and 10-10-XXX dialing out of PBX.
❑ Restrict all calls to 900, 976, 950 and 411.
❑ Restrict 1+ dialing to extent possible.
❑ Change passwords frequently.
❑ Delete/change all default passwords.
❑ Restrict after-hours calling capability: DISA, International, Caribbean and Toll calls.
❑ Analyze call detail activity daily (use SMDRs).
❑ Consider allowing only attendant-assisted international calling.
❑ Employ class-of-service screening to areas to which there is no business need to call.

❑ Restrict Toll Free dialing from areas where there is no business requirement.
❑ Frequently audit and change all active codes.
❑ Deactivate unassigned voice mailboxes and DISA codes.
❑ Do not allow phone lines to be "forwarded" to off-premises numbers.
❑ Make sure that system administration and maintenance port phone numbers are randomly selected, unlisted and that they deviate from normal sequence of other business numbers.
❑ Use random generation and maximum length for authorization codes.
❑ Deactivate all unassigned authorization codes.
❑ Use multiple levels of security on maintenance ports (if available).
❑ Do not allow generic or group authorization codes.
❑ Ensure that "Night Bell" or attendant service does not default to dial tone when left unattended.
❑ Do not use "alpha" passwords that spell common words or names.
❑ Immediately deactivate passwords and authorization codes to known terminated employees.
❑ Consider implementing a *barrier code system*, i.e. an additional numeric password that adds a second level of security.
❑ Restrict all possible means of out-dial (through-dial) capability in your voice mail system.
❑ Frequently change default codes/passwords on voice mailboxes.

More information about AT&T's NetPROTECT Family of Services may be found at: http://www.att.com/business_billing/fd_fraud2.html. You may also contact your AT&T account representative or the AT&T Service Establishment Group at 1-800-NET-SAFE.

AT&T Business Services – Global Fraud Management Organization (ABS-GFMO)
24X7 Fraud Operations Center: 800-821-8235

***NOTE**: THE INFORMATION CONTAINED IN THIS DOCUMENT IS FOR AT&T BUSINESS CUSTOMERS AND IS FOR EDUCATIONAL PURPOSES ONLY. THERE ARE NO GUARANTEES MADE WITH RESPECT TO ITS ABILITY TO PREVENT PBX FRAUD OR ASSUME LIABILITY ON THE PART OF AT&T.*

Office of Information Security
OCIO

ITPL 09-02 Segment Four Security Survey

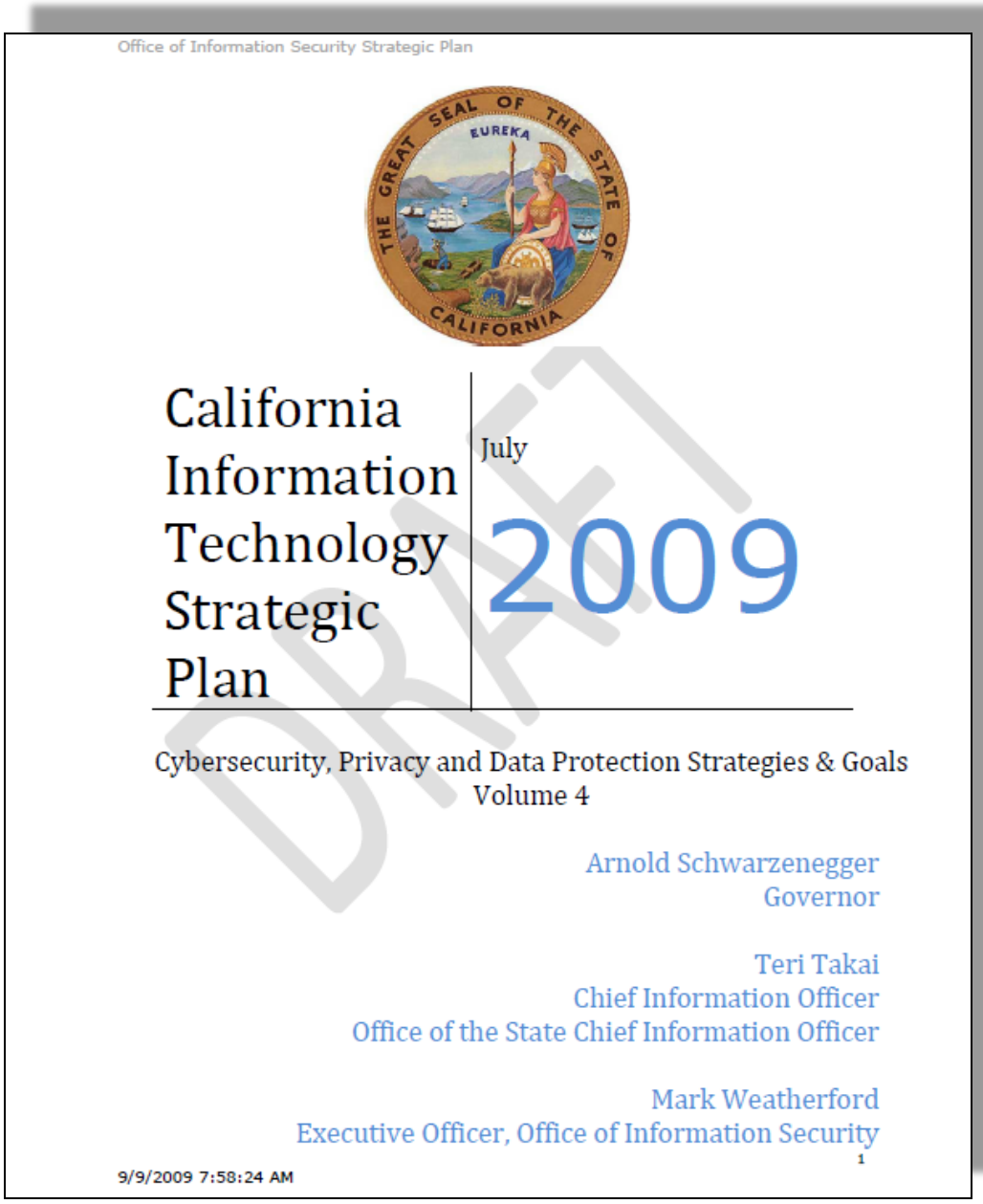
Office of Information Security
OCIO

October is Cyber-security Month

- October 13th (tentative)
- October 21th and 22th

Office of Information Security
OCIO

Strategic Plan



Office of Information Security
OCIO

Incident Management

Office of Information Security
OCIO

Why Report?

- Incident Reporting
  - A chief component of overall business risk management in any organization
  - A means of providing the agency with early warning, detection and correction of organizational process issues and system weaknesses or failures
  - Timely correction mitigates loss and risk
  - Increases state's ability to identify and address statewide security trends and gaps

Office of Information Security
OCIO

Observations & Trends

- Reporting Cost

  "*There is no such thing as a harmless attack. What is the value of the agency's brand? What would it cost to recover from a major public relations faux pas? Just because a hacker didn't steal corporate secrets or drain the payroll account doesn't mean the attack didn't cost the organization a ton of money."*

  - Jeff Crume, Author – Inside Internet Security, What Hackers Don't Want You to Know

Office of Information Security
OCIO

Observations & Trends

- Data Breaches
  - One or more of the notice triggering personal data elements identified in Civil Code Section 1798.29
  - Regardless of the type of media involved
  - Includes inadvertent loss or disclosure, and suspected and actual theft and misuse
  - Continue to rank number one
  - Handling errors continue to be the primary cause

Office of Information Security
OCIO

Observations & Trends

- Asset Loss & Theft
  - Continue to rank number two
  - Carelessness and insufficient asset management controls continue to be primary cause
  - Little to no accountability (e.g., cost recovery)
  - Other observations
    - Leaving the country
    - Not always reported, but…
      - Found on e-Bay, in lost and found at the local bar, etc.

Office of Information Security
OCIO

Observations & Trends

Website Compromises

- Continue to rank number three
- Poor coding practices continue to be primary cause
- Other causes
  - Weak passwords
  - Failure to decommission old servers/applications no longer maintained or in use

Office of Information Security
OCIO

Observations & Trends

- Malware
- Social Engineering and Phishing
- Copyright Infringement
- Compromised credentials
  - Employee/Remote user accounts
- Third-Party detection and reporting

Office of Information Security
OCIO

So What!

- What agency ISOs should be doing…
  - Identify information security program gaps when measured against current security policy and standards *(Leverage ITCP-Segment Four)*
  - Increase security awareness efforts
  - Apprise Executive Management
    - Of the problem… and
    - Recommended solution and approach
  - Engage the business in solving the problem

Office of Information Security
OCIO

So What!

- What OIS is doing (statewide efforts)…
  - Policy gap analysis and refresh
  - Online Incident Management System
  - Online Security Awareness Training
  - Threat and Vulnerability Management Program
  - Other Grant Application Projects

Office of Information Security
OCIO

Federal Grant Funds

Office of Information Security
OCIO

Security Policy

- Same 12 major topics
- First to be vetted, then published will be “Risk Management”.
- Risk Management Committee Requirement
- Supporting the policy will be accompanying standards and procedures

Office of Information Security
OCIO

Telework Policy and Security Standards Update

- DGS Telework Policy
  - DGS Telework Advisory Group (TAG)
- OIS Telework Security Standards
  - DPA will facilitate meet and confer with labor

Office of Information Security
OCIO

Social Media Policy

Recommendations:

- Have a policy on the appropriate use of social networking sites
- Ensure users are trained on the appropriate use of social networking sites, including:
  - Enabling the privacy features and disabling of "Auto-Feeds" that are not approved by your organization.
  - Not visiting un-trusted websites or follow links provided by unknown or un-trusted sources.
  - Understanding the threats posed by hypertext links, especially from un-trusted sources.
  - Following your organization's policies for incident reporting.

Office of Information Security
OCIO

Social Media Policy

Recommendations:

- Ensure that all anti-virus software is up-to-date with the latest signatures.
- Ensure that the most recent vendor patches are applied on all desktops, laptops, mobile devices and servers as soon as possible.
- Deploy network intrusion detection systems to monitor network traffic for malicious activity.

Office of Information Security
OCIO

Social Media Policy

State Direction on Departmental Use of Social Networking Media

- Agency use versus all employee use
- Argument for advantages of employee access
- Security must help business to achieve the objectives of the directive

Office of Information Security
OCIO

Closing

- Please complete the feedback survey.
- Thank you for your attendance and participation.